AO 106 (Rev. 04/10) Application for a Search Warrant AUSA Glenn-Applegate

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A White iPhone and a Gold iPhone, Currently Located at the IRS-CI Columbus Office's evidence room, 401 N. Front Street, Columbus, Ohio 43215

Case No. 2:20mj180

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment C

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 1956	Money Laundering
18 USC 1957	Money Laundering
18 USC 1343	Wire Fraud

The application is based on these facts:

See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Shawn Mincks, Special Agent, IRS-CI
Printed name and title

Sworn to before me and signed in my presence.

Date: 3-9-20

Judge's signature

City and state: Columbus, OH

Chelsey M. Vascura, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

AFFIDAVIT
IN SUPPORT OF SEARCH WARRANTS

I, Shawn Mincks, Special Agent, U.S. Department of the Treasury, Internal Revenue Service, Criminal Investigation, being duly sworn, depose and say that:

Introduction and Purpose

1. I am a Special Agent with IRS-Criminal Investigation and have been so employed since 2008. I have received specialized law enforcement training at the Federal Law Enforcement Training Center, Glynco, Georgia and additional specialized training from the IRS. My duties as a Special Agent include conducting investigations of individuals and businesses that have violated Federal Law, particularly those laws found under Title 18, Title 26 and Title 31 of the United States Code. I have participated in multiple such investigations, including several investigations related to individuals who launder funds derived from romance and other international fraud schemes.

2. I am assigned to pursue a federal criminal investigation of Robert Asante, Kwame Yeboah and other co-conspirators. I make this affidavit in support of search warrants for the following cellular phones seized by the U.S. Government during the arrests of Asante and Yeboah on March 4, 2020. These items include the following, also described in Attachments A and B:

Attachment A

a. White iPhone seized from Robert Asante;
b. Gold iPhone seized from Robert Asante.

Attachment B

a. Black iPhone seized from Kwame Yeboah;
b. Gold iPhone seized from Kwame Yeboah.

These devices are currently located at the IRS-CI Columbus Office's evidence room, 401 North Front Street, Columbus, Ohio 43215, in the Southern District of Ohio.

3. The information in this affidavit is either personally known to me based upon my experience, investigative activities, analysis of records and interviews; or it has been relayed to me by other agents and/or law enforcement personnel. This affidavit is being submitted for the limited purpose of securing search warrants, and I have not included each and every fact know to me concerning the investigation. I have set forth only the facts I believe are necessary to support the requested search warrants.

4. I contend there is probable cause to believe that Asante and Yeboah were and are engaged, together and with others, in a conspiracy to commit money laundering in violation of 18 USC 1956(h). Additionally, I contend that Asante and Yeboah each personally committed multiple acts in violation of 18 USC 1956(a)(1)(B)(i); 18 USC 1956(a)(2)(B)(i); and/or 18 USC 1957, and that evidence of such violations and evidence of wire fraud in violation of 18 USC 1343 is located on or in the items described in paragraph #2 and in Attachment A and Attachment B.

Evidence in Support of Probable Cause

5. On March 3, 2020, the affiant applied for and was granted an arrest warrant for Asante based on a Criminal Complaint alleging that Asante was engaged in a money laundering conspiracy in violation of 18 USC 1956(h). On March 4, 2020, agents with IRS-CI asked for and received assistance from the Columbus Police Department in conducting a traffic stop in order to arrest Asante. Asante was arrested while driving a black Mercedes, license plate MBAT41. When he was arrested, Asante was in possession of a white iPhone and a gold iPhone.

6. On March 3, 2020, the affiant applied for and was granted an arrest warrant for Yeboah based on Criminal Complaint alleging that Yeboah was engaged in a money laundering conspiracy in violation of 18 USC 1956(h). On March 4, 2020, agents with IRS-CI and airport police arrested Yeboah at John Glenn International airport. When he was arrested, Yeboah was in possession of a black iPhone and a gold iPhone.

7. Through interviews and analysis of bank records and other documentation, the affiant believes the investigation to date tends to show that Asante, Yeboah and others, both known and unknown, have been engaged in a conspiracy to commit money laundering in that they have knowingly and willfully facilitated the receipt, concealment and transfer of funds derived from so-called "Romance Scam" victims.

8. Perpetrators of the scams post fake profiles on various dating websites, then individuals throughout the United States and other countries are contacted by or enticed to initiate contact with the perpetrators. After contacting the victims online, the perpetrators use email, instant messaging services, text messaging and phone calls to

build a relationship of trust with the victims. Once trust is gained, the perpetrators convince the victims to provide money purportedly for various investments or need-based reasons. The perpetrators tell many of the victims that they are overseas. The perpetrators further explain, for example, that they have located a gold or diamond mine through which they can both become very wealthy if the victim invests money; have had financial trouble and need assistance; or have had legal trouble, are in prison and need money to pay off the captors. The victims then wire transfer, direct transfer or deposit money into bank accounts located within the United States and controlled by Asante, Yeboah and/or other co-conspirators. Evidence indicates that many of these bank accounts were opened in the names of business entities controlled by the co-conspirators. The victims provide the funds with the expectation that the money will be invested or used to assist their online "friend."

9. Contemporaneous and subsequent to the wire transfers, account transfers and deposits received by the co-conspirators from the victims, the co-conspirators dispose of the funds through cash withdrawals; checks issued to parties known to the co-conspirators; transfers to each other, as well as others not named in this affidavit; international and domestic wire transfers; personal expenditures; and purchases of official checks. None of the victims receive any return on their "investments" or any of their money back. The loss to all victims exceeds $7 million.

10. The affiant believes that evidence garnered so far in the investigation tends to show that the recipients of the funds, specifically Asante and Yeboah, knew that the funds they were receiving were derived from some kind of unlawful activity, and the funds were, in fact, derived from a specified unlawful activity, namely wire fraud (18 USC 1343). From the recipient bank accounts, the funds were not used in the manner promised to the victims of the fraud. Instead, the funds were transacted in a fashion designed to conceal the nature, source, location, ownership and control of the funds through cash withdrawals and other mechanisms, in violation of 18 USC 1956 (a)(1)(B)(i). Some of the transactions designed to conceal the nature, source, location, ownership and control of the funds were conducted internationally, in violation of 18 USC 1956 (a)(2)(B)(i). Additionally, many debits were in excess of $10,000, in violation of 18 USC 1957. Since they were working in concert with each other, as well as the perpetrators of the Romance Scams, the activity was in violation of 18 USC 1956(h).

Relevant Bank Accounts, Entities and Phone Numbers

11. According to bank records, Asante opened and controlled the following bank accounts, among others, in his own name and on which he was the sole signer:

a. July 30, 2014 – August 1, 2017 - PNC Bank account # xx7452 (PNC 7452).

    i. When Asante opened the account, he listed his phone number as 347-446-5619.

b. December 23, 2014 – October 10, 2017 - Bank of America account # xx9127 (BOA 9127).

c. September 9, 2015 – June 16, 2017 – JP Morgan Chase Bank account # xx3358 (JPMC 3358).

12. According to bank records, Asante's wife, Nancy Asante (Nancy), also opened and controlled an account of interest, on which she was the sole signer:

a. June 20, 2014 – May 6, 2016 – Bank of America account # xx2027 (BOA 2027).

13. According to records from the Ohio Secretary of State, Asante established Ingwet Canal LLC (Ingwet) on March 2, 2017 by filing Articles of Organization with the State of Ohio. According to bank records, he opened and controlled the following bank accounts in the name of Ingwet and on which he was the sole signer:

a. March 9, 2017 – November 30, 2017 – JP Morgan Chase Bank account # xx1215 (JPMC 1215).

b. September 14, 2018 – March 31, 2019 – TD Bank account # xx9310 (TD 9310).

    i. When Asante opened the account, he listed his phone number as 347-446-5619.

14. MoneyGram records were subpoenaed and analyzed. The records show that between March 5, 2014 and June 7, 2016, Asante sent funds numerous times to individuals in Ghana. When sending the funds, Asante used various phone numbers, including 347-446-5619.

15. According to records from the Ohio Secretary of State, Yeboah established Brightstar Automotive (Brightstar) on May 5, 2015 by filing Articles of Organization with the State of Ohio. According to bank records, he opened and controlled the following bank accounts in the name of Brightstar and on which he was the sole signer:

a. June 2, 2017 – February 2, 2018 – JP Morgan Chase Bank account # xx2366 (JPMC 2366).

b. December 18, 2017 – October 31, 2018 – Bank of America account # xx0009 (BOA 0009).

c. October 5, 2018 – at least August 31, 2019 – US Bank account # xx3133 (US 3133).

    i. When Yeboah opened the account, he listed his phone number as 347-278-0153

d. April 9, 2019 – at least August 31, 2019 – PNC Bank account # xx0518 (PNC 0518).

16. MoneyGram records show that between August 5, 2015 and April 12, 2017, Yeboah sent funds numerous times to individuals located in Ghana. When sending the funds, Yeboah used phone number 347-278-0153.

17. According to records from the Ohio Secretary of State, Asante and Yeboah established Twist Lounge & Grill (Twist) on May 26, 2016 by filing Articles of Organization with the State of Ohio. According to bank records, Asante and Yeboah subsequently opened various bank accounts in the name of Twist, including the following:

a. October 16, 2017 – March 29, 2019 – Asante and Yeboah opened and controlled JP Morgan Chase Bank account # xx5930 (JPMC 5930). Asante and Yeboah were the only two signers on the account.

b. October 10, 2018 – February 28, 2019 – Yeboah opened and controlled Bank of America account # xx7060 (BOA 7060). Yeboah was the only signer on the account.

Witness Statements and Transactions

18. According to an interview with Person 10, whose identity is known to your Affiant, Person 10 met somebody she believed to be named Nicholas Carl Hoffman on an online dating website in 2014. Hoffman convinced Person 10 that he was a middleman who facilitated international shipments, and he needed Person 10 to provide money to him for shipping fees, storage fees and taxes. Bank records show that, between

December 4, 2014 and December 19, 2014, Person 10 deposited $110,000 in cash into BOA 2027. Person 10 expected to be repaid, but she never received any of her money back.

a. Bank records show that, after receiving the funds, Asante and/or his wife engaged in numerous transactions designed to conceal the nature, source, location, and control of the funds. The transactions included, but were not limited to, issuances of checks payable to Asante totaling $68,800. Many of the checks contained memoranda stating "Car Payment."

    i. Bank records show that, of the checks issued to him, Asante deposited $17,300 into PNC 7452 where a large portion of the funds was used on personal expenditures. Asante deposited the remaining funds into a Huntington Bank account he controlled. From there, Asante sent an additional $12,000 to various individuals in Ghana. He also withdrew cash or purchased official checks totaling over $30,000.

19. Bank records show that, between January 13, 2015 and August 31, 2015, Person 10 also deposited $106,000 in cash into BOA 9127 and wired $30,500 into BOA 9127.

a. Bank records show that, after receiving the funds from Person 10 into BOA 9127, and on or about the dates set forth below, Asante engaged in the following financial transactions, among others, involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

    i. April 22, 2015 - $8,000 online banking transfer to a third party;

    ii. May 12, 2015 - $10,000 online banking transfer to a third party;

    iii. May 13, 2015 - $4,000 online banking transfer to a third party.

b. Bank records and MoneyGram records show that, after receiving the funds from Person 10 into BOA 9127, Asante transmitted funds, derived from wire fraud, from the United States to a place outside the United States and such transactions were designed to conceal the nature, source, location, ownership and control of the funds. The transactions included the following:

i. April 22, 2015 - $1,122 transaction at Wal-Mart which consisted of a MoneyGram transfer of $1,100 to Ghana plus fees;

ii. May 11, 2015 - $965.50 transaction at Wal-Mart which consisted of a MoneyGram transfer of $950 to Ghana plus fees;

iii. May 16, 2015 - $509.90 transaction at Wal-Mart which consisted of a MoneyGram transfer of $500 to Ghana plus fees;

iv. May 20, 2015 - $965.50 transaction at Wal-Mart which consisted of a MoneyGram transfer of $950 to Ghana plus fees;

v. June 9, 2015 - $1,224 transaction at Wal-Mart which consisted of a MoneyGram transfer of $1,200 to Ghana plus fees;

vi. June 9, 2015 - $1,015.50 transaction at Wal-Mart which consisted of a MoneyGram transfer of $1,000 to Ghana plus fees;

vii. June 25, 2015 - $$965.50 transaction at Wal-Mart which consisted of a MoneyGram transfer of $950 to Ghana plus fees;

viii. June 30, 2015 - $1,015.50 transaction at Wal-Mart which consisted of a MoneyGram transfer of $1,000 to Ghana plus fees;

ix. June 30, 2015 - $1,015.50 transaction at Wal-Mart which consisted of a second MoneyGram transfer of $1,000 to Ghana plus fees;

x. July 2, 2015 - $1,015.50 transaction at Wal-Mart which consisted of a MoneyGram transfer of $1,000 to Ghana plus fees;

xi. July 3, 2015 - $1,015.50 transaction at Wal-Mart which consisted of a MoneyGram transfer of $1,000 to Ghana plus fees;

xii. July 22, 2015 - $1,122 transaction at Wal-Mart which consisted of a MoneyGram transfer of $1,100 to Ghana plus fees;

xiii. July 28, 2015 - $615.50 transaction at Wal-Mart which consisted of a MoneyGram transfer of $600 to Ghana plus fees;

xiv. July 28, 2015 - $615.50 transaction at Wal-Mart which consisted of a second MoneyGram transfer of $600 to Ghana plus fees.

20. According to an interview with Person 11, whose identity is known to your Affiant, Person 11 met somebody she believed to be named Michael Gresham on an online dating website in February of 2017. Gresham told Person 11 that he was a retired Colonel and owned a business that dealt in diamonds and gold. Gresham also introduced Person 11 to Asante, with whom she communicated directly. Over time, Gresham and Asante instructed Person 11 to send money to various individuals for myriad reasons, including expenses involving a camera and a shipment of gold. Person 11 eventually discovered that the profile set up by Gresham was fake, and she had been scammed. Bank records show that, between February 21, 2017 and August 14, 2017, Person 11 deposited $68,500 in cash into BOA 9127.

a. Bank records show that, after receiving the funds from Person 11 into BOA 9127, and on or about the dates set forth below, Asante engaged in the following financial transactions, among others, involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

i. February 21, 2017 - $1,003 ATM cash withdrawal consisting of $1,000 cash plus a $3.00 fee;

ii. March 9, 2017 - $505.50 ATM cash withdrawal consisting of $500 cash plus a $5.50 fee.

21. According to an interview with Person 12, whose identity is known to your Affiant, Person 12 is a 73-year old widow who met numerous individuals online. These individuals included somebody she believed was serving in the military in the United Kingdom; somebody named Felix Dante Okoro from Ghana; and somebody she believed to be named General Stephen Townsend. Person 12 sent "hundreds of thousands of dollars" to various people at the instruction of Okoro and Townsend. An "unknown banker" instructed Person 12 to send money to Asante. Bank records show that, between July 6, 2017 and July 13, 2017, Person 12 wired $160,778 to BOA 9127.

a. Bank records show that, after receiving the funds from Person 12 into BOA 9127 and on or about the dates set forth below, Asante engaged in the following monetary transactions in criminally derived property of a value greater than $10,000:

i. July 11, 2017 - $28,600 wire to Company 12 in Ghana;

ii. July 14, 2017 - $49,850 wire to Company 12 in Ghana.

22. Bank records show that, on April 13, 2017, Person 12 wired $33,899 to JPMC 1215. The memorandum on the wire read "Goods."

a. Bank records show that, after receiving the funds from Person 12 into JPMC 1215 and on or about the date set forth below, Asante engaged in the following monetary transaction in criminally derived property of a value greater than $10,000:

i. April 14, 2017 - $25,250 wire to Company 6 in Ghana.

23. According to an interview with Person 4, whose identity is known to your Affiant, Person 4 met somebody she believed to be named Scott Bradley Hopkins on an online dating website. Hopkins told Person 4 that he needed to transport a package containing a large amount of money and jewelry to the United States. Person 4 sent approximately $300,000 to various individuals via MoneyGram, Western Union and bank wires, including somebody she believed was a military general in Ghana. She believed the funds were to be used to facilitate transport of the package. Bank records show that these funds included a wire to JPMC 1215 in the amount of $25,000 on September 26, 2017.

a. Bank records show that, after receiving the funds from Person 4 into JPMC 1215, Asante engaged in the following monetary transaction in criminally derived property of a value greater than $10,000:

i. September 26, 2017 - $20,000 wire to a company in Illinois.

24. According to an interview with Person 13, whose identity is known to your Affiant, Person 13 met somebody she believed to be named Matt Dickson on an online dating website in 2016. Dickson told Person 13 that he was a geologist who did excavation work. Dickson told Person 13 that his partner was Asante. Dickson eventually convinced Person 13 to send money to various people, including Asante. The money was supposed to be invested and used to pay for shipping fees. Person 13 was supposed to have been repaid at a rate of 10%. Bank records show that, on September 22, 2016 and September 23, 2016, Person 13 wired $25,000 and $4,000, respectively, to PNC 7452. Person 13 never received any money back.

a. Bank records show that, after receiving the funds from Person 13 into PNC 7452 and on or about the date set forth below, Asante engaged in the following monetary transaction in criminally derived property of a value greater than $10,000:

i. September 26, 2016 - $20,000 wire to an individual in Ghana.

25. Bank records show that, between January 17, 2017 and May 22, 2017, Person 13 provided an additional $148,500 to Asante, all of which was deposited into JPMC 3358.

a. Bank records show that, after receiving the additional funds from Person 13 into JPMC 3358, Asante transmitted or caused to be transmitted funds, derived from wire fraud, from the United States to a place outside the United States and such transactions were designed to conceal the nature, source, location, and control of the funds. The transactions included the following:

i. January 15, 2017 – $241.78 cash withdrawal at an ATM located in Accra, Ghana;

ii. January 18, 2017 - $482.43 cash withdrawal at an ATM located in Accra, Ghana;

iii. January 18, 2017 – a second $482.43 cash withdrawal at an ATM located in Accra, Ghana;

iv. January 19, 2017 – $479.40 cash withdrawal at an ATM located in Accra, Ghana;

v. January 19, 2017 – a second $479.40 cash withdrawal at an ATM located in Accra, Ghana;

vi. January 20, 2017 - $477.41 cash withdrawal at an ATM located in Accra, Ghana;

vii. January 20, 2017 - $474.11 cash withdrawal at an ATM located in Kumasi, Ghana;

viii. January 21, 2017 - $474.11 cash withdrawal at an ATM located in Kumasi, Ghana;

ix. January 21, 2017 – a second $474.11 cash withdrawal at an ATM located in Kumasi, Ghana;

x. January 22, 2017 – $474.11 cash withdrawal at an ATM located in Kumasi, Ghana;

xi. January 23, 2017 - $474.11 cash withdrawal at an ATM located in Kumasi, Ghana;

xii. January 26, 2017 - $475.75 cash withdrawal at an ATM located in Kumasi, Ghana;

xiii. January 30, 2017 - $476.85 cash withdrawal at an ATM located in Kumasi, Ghana;

xiv. February 1, 2017 - $471.94 cash withdrawal at an ATM located in Kumasi, Ghana;

xv. February 2, 2017 - $471.40 cash withdrawal at an ATM located in Santasi, Ghana;

xvi. February 2, 2017 – a second $471.40 cash withdrawal at an ATM located in Santasi, Ghana;

xvii. February 3, 2017 - $470.32 cash withdrawal at an ATM located in Santasi, Ghana;

xviii. February 3, 2017 – a second $470.32 cash withdrawal at an ATM located in Santasi, Ghana;

xix. February 4, 2017 - $469.25 cash withdrawal at an ATM located in Accra, Ghana;

xx. February 4, 2017 – a second $469.25 cash withdrawal at an ATM located in Accra, Ghana;

xxi. February 5, 2017 - $469.25 cash withdrawal at an ATM located in Accra, Ghana;

xxii. February 6, 2017 - $469.25 cash withdrawal at an ATM located in Accra, Ghana;

xxiii. February 6, 2017 – a second $469.25 cash withdrawal at an ATM located in Accra, Ghana.

b. Bank records show that, using funds received into JPMC 3358 from Person 13 and on or about the dates set forth below, Asante engaged in the following financial transactions, among others, involving the proceeds

of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

i. February 9, 2017 - $7,000 cash withdrawal;

ii. February 14, 2017 - $3,000 ATM cash withdrawal;

iii. February 15, 2017 - $2,000 ATM cash withdrawal;

iv. February 21, 2017 - $1,000 ATM cash withdrawal;

v. March 2, 2017 - $2,000 ATM cash withdrawal;

vi. March 7, 2017 - $3,000 ATM cash withdrawal;

vii. March 13, 2017 - $2,000 cash withdrawal;

viii. March 14, 2017 - $10,000 cash withdrawal;

ix. March 24, 2017 - $1,000 ATM cash withdrawal.

c. Bank records show that, after receiving the funds from Person 13 into JPMC 3358 and on or about the dates set forth below, Asante engaged in the following monetary transactions in criminally derived property of a value greater than $10,000;

i. February 10, 2017 - $18,000 wire to a company in Ghana;

ii. March 1, 2017 – Issuance of a check in the amount of $25,000 payable to Asante.

26. Further analysis of the bank records related to the accounts described herein show that additional funds characteristic of derivation from romance fraud were deposited and/or wired into the accounts controlled by Asante described above. Bank records relating to other bank accounts not described above were also analyzed. The additional bank records show that funds characteristic of derivation from romance fraud were deposited into these accounts as well. Not all the individuals from whom funds were received by Asante were interviewed. However, deposits from many of the individuals share characteristics with those deposits known to have originated from romance fraud. As such, funds characteristic of romance fraud which were deposited and/or wired into accounts controlled by Asante totaled at least $1.9 million. After the funds reached the

accounts, Asante engaged in transactions to dispose of the funds similar to those transactions described above, including but not limited to the following:

a. Bank records show that, between October 4, 2017 and October 5, 2017, $54,350.91 characteristic of romance fraud was received into JPMC 1215 from three different individuals. Bank records further show that, after receiving the funds, on or about October 6, 2017, Asante wired $33,626 to JPMC 2366 in the name of Brightstar Automotive.

27. According to an interview with Person 14, whose identity is known to your Affiant, Person 14 met somebody she believed to be named Rene Rehpenning who claimed to work on an oil rig in Qatar. Rehpenning eventually asked Person 14 to accept a box for him which contained $250 million. Rehpenning also claimed at one point that he had been arrested. Rehpennig and various other alleged individuals enticed Person 14 to send money related to the box of money, incarceration or other fictitious needs in order to pay fees, fines and expenses. Person 14 stated that she was defrauded out of $5 million over a period of one year. Bank records show that, on December 5, 2017, Person 14 wired $85,000 to JPMC 2366.

28. According to an interview with Person 15, whose identity is known to your Affiant, Person 15 stated that he met somebody he believed to be named Dennis Dyer on an online dating website in the fall of 2017. Dyer claimed he was in the military in Syria or Afghanistan and had amassed a significant supply of diamonds and gold. Dyer asked Person 15 for money to pay for customs and shipping fees related to shipping boxes full of these items back to the United States. Person 15 sent approximately $700,000 to various people over a two-month period at Dyer's direction. Bank records show that, on December 6, 2017, Person 15 transferred $160,000 to JPMC 2366. Person 15 expected to be repaid when Dyer came to the United States. Dyer never came to the United States, and Person 15 has not been repaid.

a. Bank records show that, after receiving the funds from Person 14 and Person 15 into JPMC 2366 and on or about the dates set forth below, Yeboah engaged in the following monetary transactions in criminally derived property of a value greater than $10,000:

i. December 6, 2017 - $50,000 wire to a bank account held in China;

ii. December 7, 2017 - $70,000 wire to Company 4 in China;

iii. December 7, 2017 - $30,000 wire to Company 3 in China;

iv. December 7, 2017 - $30,000 wire to a bank account held in Hong Kong;

v. December 7, 2017 - $20,000 wire to a company located in the United States.

29. According to an interview with the daughter of Person 6, whose identity is known to your Affiant, Person 6 has been admitted to a psychiatric ward because of scams perpetrated upon him by various individuals known to Person 6 as Jack Renteria and Diplomat Keith Harper. Person 6 lost $800,000 due to these scams. Bank records show that Person 6 deposited $24,900 in cash into BOA 0009 on February 23, 2018.

30. According to an interview with the daughter of Person 9, whose identity is known to your Affiant, Person 9 met somebody he believed to be named Roger Snider on an online dating website in December of 2017. Snider told Person 9 that he was a soldier serving in Syria. Snider told Person 9 he had saved a woman's life, and a rich oil barren wanted to reward him by paying him $2 million in gold. Person 9 provided a total of approximately $471,000 to numerous people at Snider's direction related to a supposed package containing the $2 million in gold. Bank records show that these funds included wires totaling $58,400 to BOA 0009 on January 22, 2018 and January 23, 2018.

a. Bank records show that, after receiving the funds from Person 6 and Person 9 into BOA 0009 and on or about the dates set forth below, Yeboah engaged in the following monetary transactions in criminally derived property of a value greater than $10,000:

i. January 25, 2018 - $25,000 wire to Company 3 in China;

ii. February 27, 2018 - $22,850 wire to Company 3 in China

b. Bank records show that, after receiving the funds from Person 6 and Person 9 into BOA 0009 and on or about the dates set forth below, Yeboah engaged in the following financial transactions, among others, involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

i. January 24, 2018 - transfer of $5,000 to Conspirator 8;

ii. January 24, 2018 – transfer of $7,500 to Conspirator 7.

iii. Wires and a check totaling $32,100 to Asante;

1. Bank records show that Asante received the funds into a Navy Federal Credit Union account he controlled. Between January 25, 2018, when the first funds were deposited, and May 17, 2018, when most funds were depleted, Asante withdrew $5,400 in cash via ATMs in Ghana; sent over $28,000 to various individuals via Peer 2 Peer transfers; and disposed of a significant portion through personal expenditures.

31. According to an interview with Person 16, whose identity is known to your Affiant, Person 16 stated that, after her husband died, she received an unsolicited social media message from somebody she believed to be named Ben Grayson. Grayson told Person 16 that he was in the army in Afghanistan. Eventually, Grayson asked Person 16 to send him money to pay for fees and costs associated with shipping a box from Afghanistan to the United States. Later, Grayson told Person 16 that he needed money to help pay for his transportation back to the United States. Person 16 sent money to various places at his request and expected to be repaid. Bank records show that, on May 23, 2019, Person 16 wired $18,000 to PNC 0518. Grayson did not travel to the United States, and a box never arrived from Afghanistan. Person 16's money has not been returned to her.

a. Bank records show that, after receiving the funds from Person 16 into PNC 0518 and on or about the dates set forth below, Yeboah engaged in the following financial transactions, among others, involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

i. May 24, 2019 - $8,000 cash withdrawal;

ii. May 28, 2019 - $6,000 cash withdrawal;

32. Bank records show that Person 16 also wired $40,000 to US 3133 on May 15, 2019.

a. Bank records show that, after receiving the funds from Person 16 into US 3133 and on or about the date set forth below, Yeboah engaged in the following monetary transaction in criminally derived property of a value greater than $10,000:

i. May 21, 2019 - $41,571 withdrawal, which consisted of the purchase of seven official checks payable to automobile auction companies.

33. According to an interview with Person 23, whose identity is known to your Affiant, Person 23 met some people on a social media application. Eventually, the people convinced Person 23 to send money to them to pay for fees related to the shipment of a box of valuables into the United States. Person 23 eventually realized she was being defrauded and reported the scam to the FBI in early 2019. Bank records show that, on November 2, 2018, Person 23 wired $90,000 to BOA 7060.

a. Bank records show that, after receiving the funds from Person 23 and other funds characteristic of derivation from romance fraud and on or about the date set forth below, Yeboah engaged in the following monetary transaction in criminally derived property of a value greater than $10,000:

i. December 20, 2018 – $59,400 wire to Robert Asante at Ecobank Ghana.

34. Further analysis of the bank records related to the accounts described herein show that additional funds characteristic of derivation from romance fraud were deposited and/or wired into the accounts controlled by Yeboah described above. Bank records relating to other bank accounts not described above were also analyzed. The additional bank records show that funds characteristic of derivation from romance fraud were deposited into these accounts as well. Not all the individuals from whom funds were received by Yeboah were interviewed. However, deposits from many of the individuals share characteristics with those deposits known to have originated from romance fraud. As such, funds characteristic of romance fraud which were deposited and/or wired into accounts controlled by Yeboah totaled at least $1.2 million. After the funds reached the accounts, Yeboah engaged in transactions to dispose of the funds similar to those transactions described above.

Conspirator 6

35. When he was arrested on March 4, 2020, Asante asked permission to call his girlfriend to take custody of his child and his vehicle. Asante's girlfriend arrived on the scene and was identified. Ohio Secretary of State records show that Asante's girlfriend established Company 7 in September of 2018. Confidential sources indicate that Asante's girlfriend received funds characteristic of derivation from romance fraud totaling almost $550,000 between October of 2018 and August of 2019. The funds Asante's girlfriend received included $275,000 from Person 23. As described in

paragraph #33, Person 23 also sent funds to Yeboah. After receiving the funds, Asante's girlfriend wired a portion of the funds to a company to which Yeboah had also wired funds in October of 2018. Asante's girlfriend also received money from and/or sent money to JPMC 5930 and US 3133.

Use of Electronic Devices

36. I contend that Asante, Yeboah and others use various electronic devices to communicate with each other and other co-conspirators regarding and in facilitation of the fraud schemes and money laundering activities. This contention is based upon witness statements through which I learned that the victims in this investigation communicated with the perpetrators via email, instant messaging services, text messaging and phone calls. These forms of communication are often accessed through electronic devices, including cell phones. At least one victim stated that she had communicated with Asante directly using these media. This contention is further based upon additional investigative experience and other specific information obtained during the investigation, including the information in the following sections.

Pen Register and Trap and Trace

37. Between September 20, 2019 and November 14, 2019, IRS-CI also placed pen registers and trap and trace devices on WhatsApp phone numbers 347-446-5619 (associated with Asante) and 347-278-0153 (associated with Yeboah).

38. I know from investigative experience that WhatsApp is a smart phone application which can also be accessed via a computer. WhatsApp is a free instant messaging and voice over internet protocol service. The user of the application downloads the application to their phone and/or computer, and the application requires the user to assign a phone number to the application. After a phone number is assigned to the application, the application sends a verification text to the phone number assigned. In this way, the application is linked to the phone number of the phone onto which the application was downloaded.

39. I also know that smart phone applications such as WhatsApp are often installed on the phones of the perpetrators of fraud schemes such as this. This application is used by persons engaged in fraud to communicate with individuals while potentially disguising their true identities. These communications can include communications with co-conspirators as well as victims.

40. The Pen Registers and Traps and Traces revealed that both of the phone numbers were active throughout the time period. It further revealed that Asante and Yeboah

were in frequent communication with each other as well as numerous phone numbers based in Ghana throughout the monitored time period. Communications sent and received included text messages, audio files, video files and image files.

41. The Pen Registers and Traps and Traces revealed that the phone or phones being used by both Asante and Yeboah to send outgoing messages via WhatsApp were iPhones.

Conspirator 1, Conspirator 5 and Conspirator 9

42. From at least April of 2012 through February of 2018, Conspirator 9 and others engaged in a conspiracy to commit money laundering in that they knowingly and willfully facilitated the receipt and transfer of funds derived from so-called "Romance Scam" victims. On February 14, 2018, Conspirator 9 was arrested following the filing of a criminal complaint related to this activity. On March 1, 2018, a grand jury returned an indictment charging Conspirator 9 and others with numerous counts in violation of money laundering statutes. Conspirator 9 has since pled guilty to violations of 18 USC 1956(h) and is currently serving a prison sentence.

43. When Conspirator 9 was arrested on February 14, 2018, his iPhone was seized and subsequently searched pursuant to a search warrant. The search of the phone revealed that Conspirator 9 was involved in two separate communication strings via the communication application WhatsApp with Conspirator 5 in Ghana and somebody later identified by Conspirator 9 to be Conspirator 1.

44. In the WhatsApp exchanges found on Conspirator 9's phone, Conspirator 5 and Conspirator 9 engage in communications, and sometimes Conspirator 9 relays the content of these discussions to Conspirator 1.

45. Bank records show that Conspirator 1 controlled a JP Morgan Chase Bank account (JPMC Account A) between at least the time period June of 2016 and February of 2018. Bank records further show that the account received over $1,131,000 in funds from several people in the United States and Canada during this time period. Notes related to incoming wires include such memoranda as "Payment for Holiday," "Purchase Property," "Other Investment," and "Goods." I interviewed nine of the individuals from whom Conspirator 1 received funds totaling over $864,000, including Person 8 who wired $29,000 to JPMC Account A on or about January 22, 2018. The statements they made regarding the nature of the money provided to Conspirator 1 was similar to the information provided by the individuals described previously in this affidavit and who provided funds to Asante and Yeboah. The deposits comprising the remaining approximately $450,000 were also characteristic of derivation from romance fraud.

46. Bank records show that, after receiving the funds from those nine people, as well as others, Conspirator 1 disposed of the funds largely through cash withdrawals; domestic and international wires/transfers; and purchases of official checks. This is similar to the activity in which Asante and Yeboah engaged after receiving funds into the bank accounts they controlled.

47. Comparison of activity in JPMC Account A to the WhatsApp conversations revealed that the discussions between Conspirator 5 and Conspirator 9 and subsequent relays of these conversations from Conspirator 9 to Conspirator 1 correspond to transactions occurring in JPMC Account A. Some of these conversations include the following:

a. On January 22, 2018, Conspirator 5 sent Conspirator 9 a message containing an attachment. The attachment was a screenshot of a wire transfer from Person 8 to JPMC Account A in the amount of $29,000. Bank records show that Person 8 sent a $29,000 wire to JPMC Account A on or about January 22, 2018.

b. On January 22, 2018, Conspirator 5 sent Conspirator 9 a communication with the information "Bank of America; New York, NY 10017; (Conspirator 2); $7700." JPMC Account A records show that on January 22, 2018, $7700 was wired from JPMC Account A to Conspirator 2.

c. On January 22, 2018, Conspirator 5 sent Conspirator 9 a communication with the information "Bank of America; (Conspirator 3); $8600." JPMC Account A records show that on January 24, 2018, $8600 was wired from JPMC Account A to Conspirator 3.

d. On January 23, 2018 at 1:37AM UTC, Conspirator 5 sent Conspirator 9 a communication with the information "Bank of America; Name on Account: (Conspirator 4)." The communication also contained an address, account number and routing number. On January 23, 2018 at 11:49AM UTC, Conspirator 9 sent Conspirator 1 a communication with the same information. Bank records show that on January 23, 2018, $10,000 was wired from JPMC Account A to Conspirator 4.

e. On January 23, 2018 at 12:28PM UTC, Conspirator 5 sent Conspirator 9 a communication with the information "(Company 1); 7385 chase (sic)." The communication also contained an account number. On January 23, 2018 at 1:19PM UTC, Conspirator 9 sent Conspirator 1 a communication with the same information. Bank records show that on January 23, 2018, a

check was issued from JPMC Account A to Company 1 in the amount of $7385.

f. On January 23, 2018, Conspirator 5 sent Conspirator 9 a message containing an image of bank information for Company 3 in China. This is the same Company 3 to which Yeboah sent wires in December of 2017 and January and February of 2018. Conspirator 5 followed that message with two additional messages stating "Any amount can go" and "$30K and above."

g. On January 26, 2018, Conspirator 1 sent Conspirator 9 a message containing an image of a wire transfer confirmation in the amount of $30,000 from JPMC Account A to Company 3. Bank records show that a wire in the amount of $30,000 was sent from JPMC Account A to Company 3 on or about January 26, 2018.

h. On February 5, 2018, Conspirator 5 sent Conspirator 9 a message with an attachment showing bank account information for Company 4 in China followed later by a message stating "50 k for China." This is the same Company 4 to which Yeboah sent a $70,000 wire on December 7, 2017.

i. On February 5, 2018, Conspirator 9 sent Conspirator 1 a message stating "I need u to do China ooo" followed by a message stating "50" and a third message containing the same image that Conspirator 9 had received from Conspirator 5 with the information related to Company 4.

j. On February 5, 2018, Conspirator 1 sent Conspirator 9 a message containing an image of a wire confirmation showing that he had wired $50,000 from JPMC Account A to Company 4. Bank records show that a wire in the amount of $50,000 was sent from JPMC Account A to Company 4 on or about February 5, 2018.

k. On February 5, 2018, Conspirator 9 sent Conspirator 5 a message containing an image of a screen grab showing that JPMC Account A had wired $50,000 to Company 4.

48. Conspirator 9's iPhone also contained a WhatsApp conversation between Conspirator 9 and phone number 347-446-5619. The person to whom phone number 347-446-5619 belonged was identified in the phone as "Jigga old." Conspirator 9 told investigators that Asante's nickname is Jigga.

49. Conspirator 9 told investigators that Conspirator 5 defrauds people throughout the world and receives money into numerous accounts he controls. Conspirator 9 told investigators that Conspirator 5 often sent him messages regarding fraudulent financial transactions involving Conspirator 1 and/or Asante. Conspirator 9 stated that he would routinely relay information from Conspirator 5 to Conspirator 1 and/or Asante with respect to the transactions. Conspirator 9 stated that Conspirator 1 and Asante knew that the money being sent to their accounts was "bad money."

50. Conspirator 9's iPhone also contained a WhatsApp conversation between Conspirator 9 and phone number 233-552-512-359. The person to whom phone number 233-552-512-359 was identified in the phone as "Jigga Gh." Phone numbers beginning in "233" are Ghanaian phone numbers. In the conversation, Asante made statements confirming a relationship between Conspirator 5, Conspirator 9 and Asante.

51. Conspirator 9 also told investigators that Asante brought Yeboah into the activity described in this affidavit. Conspirator 9 knows this because Asante told him that he had Yeboah transfer money for him.

Technical Background

52. I have consulted with IRS-CI Special Agent-Computer Investigative Specialist Dennis Nutt regarding the aspects of properly retrieving and analyzing electronically stored computer data. Special Agent Nutt has been employed with IRS-CI since 1988. In addition to attending training in financial investigation techniques and accounting, he has also completed the IRS-CI Basic Computer Evidence Recovery Training class at the Federal Law Enforcement Training Center in Glynco, Georgia, (2006), the Advanced Computer Evidence Recovery Training class at the CyberCrimes Center in Fairfax, Virginia (2007, 2012, 2016, and 2018), Macintosh Forensics Training in Glynco, Georgia (2016), and Basic Computer Forensics Examiner Training – International Association of Computer Investigative Specialists in Orlando, Florida (2018) where he learned about the operation of computer systems and the correct procedures for seizure and analysis of computer systems. Special Agent Nutt has also completed the Mobile Device Forensics Training in Glynco, Georgia (2014) and the Advanced Mobile Device Forensics Training in Glynco, Georgia (2016) where he learned about the operation of mobile devices and the correct procedures for seizing and analyzing those devices.

53. During the last 14 years Special Agent Nutt has participated in scores of search warrants during which he has seized numerous computers and has been responsible for analyzing seized electronic data and records from those systems.

54. Based upon the affiant's consultation with Special Agent Nutt, the affiant knows that searching and seizing information from computers often requires agents to seize most or all electronic storage devices to be imaged and searched later by a qualified computer specialist in a laboratory or other controlled environment. This requirement is due to the following:

a. Technical requirements: Images or backups of computer data need to be restored to a separate computer and verified to ensure that the files restore or copy properly. Additionally, evidence may be encrypted, password protected, or may be in a format that could result in evidence being overwritten and/or destroyed electronically should an attempt be made to examine the electronic evidence on site.

b. The volume and nature of electronic evidence: A seemingly small media storage device can store the equivalent of thousands of pages of information or more. It may be impractical to attempt data analysis on site.

c. The terms "records", "documents", and "materials" as used above include all of the items of evidence more fully described in Attachments C and D in whatever form and by whatever means such records, documents, or materials, their drafts, or their modifications may have been created or stored, including, but not limited to any handmade form (such as writing, drawing, painting, with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any electrical or magnetic form (such as tape recording, cassettes, compact disks); and/or any information on an electronic, digital, or magnetic storage device (such as floppy diskettes, hard drives, USB drives, backup media, disk cartridges, CD-ROMs, DVDs, optical disks, smart cards, cell phones, tablets, or electronic notebooks); as well as printouts or readouts from any magnetic storage device.

55. The warrant I am applying for would permit law enforcement to compel certain individuals to unlock a device subject to seizure pursuant to this warrant using the device's biometric features. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These

biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or

alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device.

i. Due to the foregoing, if the device that is subject to seizure pursuant to this warrant may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of Asante or Yeboah to the fingerprint scanner of the device; (2) hold the device in front of the face of Asante or Yeboah to activate the facial recognition feature; and/or (3) hold the device in front of the face of Asante or Yeboah and activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

Conclusion

56. Based on the information presented in this affidavit, I contend that Asante, Yeboah and others are engaged in a conspiracy to commit money laundering in violation of 18 USC 1956(h). I further contend that Asante, Yeboah and others have each personally committed multiple acts in violation of 18 USC 1956(a)(1)(B)(i); 18 USC(a)(2)(B)(i); and/or 18 USC 1957 in furtherance of the conspiracy. I further believe that Asante, Yeboah, and others use various electronic devices to communicate regarding and to facilitate the laundering of funds derived from fraud schemes, and evidence of these violations, as well as violations of 18 USC 1343, is now located in the items described in Attachments A and B. Because these warrants seek only permission to examine devices already in law enforcement's possession, the execution of these warrants do not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Shawn A. Mincks
Special Agent, IRS-CI

Subscribed and sworn to before me

This 9 day of March, 2020.

THE HONORABLE CHELSEY M. VASCURA
United States Magistrate Judge

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF
THE SEARCH OF:

NO. 2:20 mj 180

A White iPhone and a Gold iPhone, Currently Located at the IRS-CI Columbus Office's evidence room, 401 N. Front Street, Columbus, Ohio 43215.

ATTACHMENT A: LOCATION TO BE SEARCHED

Two iPhones seized by IRS-Criminal Investigation from Robert Asante when he was arrested on March 4, 2020, and which are currently located at the IRS-CI Columbus Office's evidence room, 401 N. Front Street, Columbus, Ohio 43215. The two iPhones are further described as follows:

a. White iPhone
b. Gold iPhone

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF
THE SEARCH OF:

NO. 2:20 mj 180

A White iPhone and a Gold iPhone, Currently Located at the IRS-CI Columbus Office's evidence room, 401 N. Front Street, Columbus, Ohio 43215.

ATTACHMENT C: ITEMS TO BE SEIZED

Information to be seized by the government:

1. All information that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud); any section of 18 U.S.C. § 1956 (money laundering) and/or 18 U.S.C. § 1957 (money laundering), regardless of the format in which they are or may be stored, for the period December 1, 2014 to the present, including but not limited to:

   a. Evidence of user attribution showing who used or owned computers, cell phones, and electronic devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

   b. Records identifying the establishment, ownership, operation and/or control of any limited liability corporation or other business entity including articles of organization; correspondence with and/or submissions to/from any Secretary of State office; applications, disposition records and/or correspondence related to the issuance or use of Employer Identification Numbers (EIN); minutes and other official business records; and documents identifying any registered agent(s), incorporator(s), and/or other identified members;

   c. All records related to offered or actual purchase, sale, transfer or shipment of motor vehicles or other consumer goods including sale advertisements or listings, correspondence, purchase orders, contracts, invoices, receipts, vehicle registrations, titles, shipping records, and delivery notices;

   d. All records related to or referencing electronic transfers of funds or cash deposits including requests for an electronic transfer or cash deposit, wiring or deposit instructions, receipts, and correspondence;

   e. All records related or referring to persons or entities in other countries and the locations of such persons entities;

   f. Asset ownership and/or acquisition records including contracts, invoices, receipts,

registrations, titles insurance records and/or photographs of assets including motor vehicles, real property, boats, jewelry, precious metals and gems, and currency (foreign, domestic, or virtual currency);

g. Travel records including travel directions, hotel reservations, rental car reservations, airplane reservations, invoices, airline tickets, and itineraries;

h. Records related to banking activity including communications and data related to the opening, closing, use, custody and/or control of bank accounts, alternative currency accounts (i.e. those related to Bitcoins), credit cards, and/or debit cards including applications for accounts; approval or declination notices; credit and/or debit card issuance notices; credit and/or debit card activations; bank statements; welcome or account opening/closing notifications; deposit, payment, withdrawal, or transfer orders, receipts and/or notifications; balance inquiries and/or notices; and security notifications;

i. All financial statements, accounting records and supporting source documents relating to receipts, expenditures, general ledgers, accounts and notes receivable, accounts and notes payable, balance sheets, income statements, statements of profit and loss, and any other accounting records and other records and/or ledgers relating to Brightstar Automotive, Ingwet Canal, or any variation of these entity names or any other entities identified through items seized pursuant to section b. above;

j. Records pertaining to any financial institution account including but not limited to account numbers, passwords, personal identification numbers (PINS), deposit/withdrawal records, notes, logs, and photographs;

k. Electronic records of internet sites visited and data accessed and/or communications made in the course of visiting such internet sites;

l. Communications records and histories made through and/or from applications (known as "Apps"); emails; texts; calls or other media contained on the electronic devices to be searched and all attachments included in such communications; and

m. Contact lists and any documents reflecting names, addresses, email addresses, telephone numbers, fax numbers and/or other contact information.